Docket No.: SON-2320
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Makoto OKA et al.

Confirmation No.: 4260

Application No.: 10/041,964

Art Unit: 2134

Filed: January 9, 2002

Examiner: W. S. Powers

For: PUBLIC KEY CERTIFICATE ISSUING SYSTEM, PUBLIC KEY CERTIFICATE ISSUING METHOD, DIGITAL CERTIFICATION APPARATUS, AND PROGRAM STORAGE MEDIUM

REPLY BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is a Reply Brief under 37 C.F.R. §41.41 in response to the Examiner's Answer mailed on November 27, 2007.

All arguments presented within the Appeal Brief of April 12, 2007 are incorporated herein by reference. Additional arguments are provided below.

STATUS OF CLAIMS:

Claims 1-36 are present within the above-identified application, with claims 1, 14, 23, and 36 being independent. No claims have been allowed.

GROUNDS OF REJECTION:

Within the Final Office Action of February 7, 2007:

Page 2 of the Final Office Action includes a rejection of claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32, and 34-36 under 35 U.S.C. § 102(b) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al.

Page 3 of the Final Office Action includes a rejection of claims 4, 7, 26, and 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of U.S. Patent No. 6,202,157 to Brownlie et al.

Page 3 of the Final Office Action includes a rejection of claims 8, 18, and 30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of "On the Importance of Checking Cryptographic Protocols for Faults" by Boneh et al.

Page 4 of the Final Office Action includes a rejection of claims 11, 21, and 33 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. in view of U.S. Patent No. 6,675,296 to Boeyen et al.

In the Appeal Brief mentioned above, Appellants provided various arguments countering these grounds of rejection, and the arguments found in the Brief are incorporated herein.

ARGUMENT

In the Office Action of February 7, 2007:

The Final Office Action erroneously rejects claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32, and 34-36 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,035,402 to Vaeth et al. ("Vaeth").

Claims 1-3, 9, 10, 12, and 13

Claims 2, 3, 9, 10, 12, and 13 depend on claim 1. Claim 1 recites:

A public key certificate issuing system comprising:

a certificate authority for issuing a public key certificate used by an entity; and
a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;
wherein said certificate authority, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

These claimed features are neither disclosed nor suggested by Vaeth. As previously noted, Vaeth arguably discloses a Virtual Certificate Authority where requests for a certificate and verification information are directed to the Certificate Authority (CA) from a plurality of entities, directly or through a Registration Authority (RA), acting as a "virtual CA" (VCA).

Vaeth discloses a three-entity relationship used to produce certificates. At the top-tier of the hierarchy is the Certification Authority (CA). At the bottom-tier are the entities (Vaeth, Fig. 3: elements 170, 178, 179) which requests certificates via certificate request and data (CRDs). An Entity will issue a request for a certificate through a Registration Authority (RA) (Vaeth, Fig. 3: elements 180) or directly to the Certification Authority (CA) (Vaeth, Fig. 3: elements 190). The RA is positioned in the middle-tier, in one of two capacities. In a first capacity the RA will retrieve requests from the CA and verify the entities making the requests (Vaeth at 7:48-51). In a second capacity, as a virtual CA, the RA will receive certificate requests from an Entity and relay the request to the CA, once the RA verifies the entity (Vaeth at 7:58-63).

The CA uses generic or specialized cryptography functions from a combination of crypto-cards to produce different types of certificates (Vaeth, Fig. 3: elements 246-249, and at 7:36-40). The CA employs a particular combination of generic or specialized certificate functions, based on the requesting Entity, to produce a certificate (Vaeth at 7:36-40). The combination of generic or specialized certificate functions employed by the CA is directly dependent on the requesting Entity.

The CA produces each type of certificate based on the association between certificate types and requesting entities.

Vaeth fails to disclose an explicit association between the RA used to verify a given certificate request and the type of certificates the CA issues. The type of certificate the CA issues is determined by the requesting entity. This allows a given entity to make a request for the same type of certificate through multiple RAs, and for the implementation of schemes wherein a single entity can obtain similar types of certificates through one or multiple RAs. (Vaeth, Fig. 3: elements 180 and 188, and at 8:52-59).

In Vaeth, a CA may be configured to provide specialized functions for each entity, such as for cardholders, merchants, and payment gateways (Vaeth at 7:30-35). The CA uses a variety of crypto-cards that respectively perform cryptographic functions, including the generation of the particular type of certificate. However, the CA only executes the crypto-cards associated *with a given type of entity to produce a given certificate.* (Vaeth at 7:34-47).

There is no mention or suggestion that the applicable crypto-card is based on the RA associated with a given requesting entity. These different cryptographic functions, provided by the crypto-cards of Vaeth, are apparently directed at the general differences that are required for the *different roles of the entities*. For example, the functions provided by the CA may be different for a cardholder as opposed to a merchant.

On page 6, **the Examiner's Answer** asserts that Vaeth teaches:

wherein said certificate authority, having a plurality of signature modules (crypto cards) *each executing a different encryption algorithm* (column 7, lines 41-47), *selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with an the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate* (Different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate.) (column 7, lines 41-47 and column 8, line 35-column 9, line 12).

On page 15, the **Examiner's Answer** argues that the:

> "different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate."

However, the Examiner's Answer fails to identify how "verify[ing] the certificate request of the users through a registration database" is equivalent the RA being associated with a "user, crypto card and private keys." Instead, it appears as though the RA simply provides verification of the user, not any information relating to the form of

encryption and keys used, and therefore does not directly associate the RA with the encryption when the encryption key is applied to the digital signature.

On page 15, the **Examiner's Answer** maintains that the RA is not a generic entity and that the crypto-card used is clearly based on the requesting RA. The Examiner's Answer cites to column 7, lines 23-38 of Vaeth, claiming that Vaeth espressly states that "a Registration Authority (RA) may be associated with a credit card issuer while another RA may be associated with a corporate account authorization office."

First, RAs exist as parts of a business. As such, all RAs are related to some kind of business or function. In the embodiment set forth in Vaeth, one RA is a card issuer while another is a corporate account authorization office. The issue is whether, when a request is actually made for a digital signature vand public key, the entity making the request through the RA triggers the applicable crypto-card or whether the RA triggers the applicable crypto-card. Restated, the issue is whether the originator of the request (the entity requesting the signature and key) triggers the applicable crypto-card, or whether the intermediate entity (the RA) triggers the applicable crypto-card.

While Vaeth discloses that the RAs may be a credit card issuer, corporate account authorization office or any other association, this does not refute the position set forth in the appeal that these associations do not determine the type of crypto-card used by the CA. That is, the entity relationship that decides which certification scheme is the CA, because the CA issues the signature and key based on the requesting entity not on the RA's function. It is the entity requesting the signature and key that determines the type of digital signature and key it receives.

At Column 7, line 33-40, Vaeth recites:

> FIG. 4 is a block procedural flow diagram for certificate issuance in the above system for *user 170*. A similar procedure could be used for different types of certificates for *merchant 177 or payment gateway 178*. Within the preferred

> embodiment of the on-line CA system 220, the procedures are implemented in software through generic certificate request server application functions 221 and specialized functions, for example, for *cardholders 222, merchants 223, and payment gateways 224.*

This portion of Vaeth, supports the position that the type of certificate issued by the CA is only based on the requesting entity (e.g., "*cardholders 222, merchants 223, and payment gateways 224")*. This allows a given entity to make a request for the same type of certificate through multiple RAs, and for the implementation of architectures wherein a single entity can obtain similar types of certificates through one or multiple RAs, or where multiple RAs verify a given entity. (Vaeth, Fig. 3: elements 180 and 188, and at 8:52-59).

On page 15, the **Examiner's Answer** further argues that during certificate creation,

> [t]he RAs act as "virtual CAs" (Vaeth, column 7, lines 64-65), and although a single RA can be used for approval of three different types of certificates (Vaeth, column 9, lines 5-9), the RA acts as a different "virtual CA" to the CA for each of the different kinds of approval. The RA, in affect, assumes the role of the requestor in the approval scheme and causes the CA to apply the appropriate digital signature executed by the various cryptographic cards (crypto cards) in the CA of Vaeth."

Vaeth discloses that an RA can act as a "virtual CA" (Vaeth at 7:59- 8:6). In this capacity the RA simply provides verification of certificate request and data (CRD) from the entity, and relays the information from the entity to the CA. This allows the RA to hide the fact that it is acting as an intermediary by making the CA invisible to the entity. However, nowhere does Vaeth contradict the position that within "the on-line CA system 220, the [cryptography] procedures are implemented in software through generic certificate request server application functions 221 and specialized functions, for example, for [the entities which comprise the] *cardholders 222, merchants 223, and payment gateways 224.*"

On page 16, the **Examiner's Answer** asserts that Vaeth discloses "'a table that associates the registration authority with the assigned encryption algorithm" because "[t]he Examiner *sees* the table of the instant application as a representation of an association between a registration authority and a signature algorithm. As such, Vaeth does teach an association between a registration authority and a signature algorithm in the form of a crypto card."

> A claim is anticipated only if *each and every element* as set forth in the claim is found, *either expressly or inherently* described, in a **single** prior art reference.
> *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Claim 1 recites "*a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.*"

In setting forth the rejection of claim 1, the Examiner's Answer fails to identify a comparable feature, and simply cites an abstraction not disclosed in the reference. Vaeth does not explicitly disclose how the relationship between entity and crypto-card is stored. The Federal Circuit has set forth that the "[e]xclusion of any claimed feature from consideration is also deemed improper." *In re Lowry*, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994)(Board erred by denying patentable weight to data structure limitations). Similarly, the Federal Circuit has set forth that "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As such, with respect the claimed "table," the Examiner's response fails to satisfy the requirements of anticipation.

Accordingly, Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on the requesting Registration Authority (RA).

- *Thus, Vaeth fails to disclose, teach or suggest wherein said certificate authority, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digita signature to message data constituting a public key certificate.*

Claims 5

In Vaeth, the Certification Authority (CA) produces the type of certificates based on the requesting entities, not based on signature module information from the RA.

Page 5 of the Final Office Action cites to Vaeth at 7:41-47 and 8:49-9:12, as a basis that Vaeth discloses that the RA management data includes signature module information applicable to the signatures.

However, Vaeth only discloses that the CA uses multiple crypto-cards, and Vaeth clearly teaches that multiple entities can use the same RA to request different types of certificates from the Certification Authority (CA) (Vaeth at at 7:41-47 and 8:49-9:12). The CA produces the type of certificates based on the requesting entities (Vaeth at 9:5-9). Vaeth discloses that a given entity can make requests through different RAs, particularly because the type of certificate does not depend on the intermediate RA (Vaeth at 9:8-12). That is, Vaeth does not disclose that the type of certificate issued by the CA is based on the RA authenticating a given entity.

On page 17, the **Examiner's Answer** states that "[t]here is nothing in the claim language that requires the RA to be associated with only one signature module or that the RA cannot request different types of certificates" (Page 17). Furthermore, the Examiner's Answer states that "[e]ven if the Vaeth patent restricted all entities to go through one RA to request certificates from a CA, the RA differentiates itself to the CA by "acting as a different 'virtual CA'".

Claim 5 depends on claim 1 and 3, which limits the associations available to each RA as being a one-to-one relationship. In particular, claim 1 recites "*based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that* ***associates the registration authority with the assigned encryption algorithm.***" The claim does not address pluralities of RAs or pluralities of encryption algorithms. Furthermore, the fact that RAs in Vaeth may act as "virtual CAs" does not change the fact of the nature of the interactions change the relationship between the entities, the CA, and the type of certificate issued.

Claim 3 builds on this position reciting "*a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with* ***a encryption algorithm specific to each of said registration authorities.***" Claim 5 applies these limitation to the actual signatures themselves, essentially creating a one-to-one relationship between signatures and RAs.

- *Thus, Vaeth fails to disclose, teach or suggest wherein said registration authority management data includes signature module identification information applicable to signatures.*

Claims 6 and 7

Vaeth does not disclose using information from the RA to determine which encryption algorithm to use to produce a given type of certificate.

Page 7 of the Final Office Action cites to Vaeth at 7:41-47 and 8:49-9:12, as a basis that Vaeth discloses that the RA transmits encryption algorithm designation information along with said public key certificate issuance request.

On page 16, the **Examiner's Answer** states that "[t]he RAs of Vaeth act as 'virtual CAs' (Vaeth, column 7, lines 64-65) and as such convey information supplied by the requesting entity to CA for the appropriate certificate with the appropriate signature. In Vaeth, there are different

functions for cardholders, merchants and payment gateways and they require different crypto cards to generate the needed certificates (Vaeth, column 7, lines 33-47)" (Page 17-18).

While Appellant agrees that the CA performs different functions depending on whether the requesting entities are cardholders, merchants, or payment gateways, the authorizing entity granting the certificate is the CA. Even in cases where the RA is acting as a "virtual CA," the CA determines and issues the certificate (Vaeth at 8:34-47), not the RA. In this embodiment, when the RA acts as a "virtual CA," the RA relays CRD and certificates between the entity and the CA, performing any necessary verification of the entity before allowing the CA to grant the appropriate certificate.

As disclosed above, Vaeth does not disclose employing information from an RA to decide which crypto-card to use to produce a given certificate. While Vaeth uses the RA to decide whether an entity is *authorized* to make a request, Vaeth does not indicate that the *authorization* includes *encryption algorithm designation information.*

- *Thus, Vaeth fails to disclose, teach or suggest wherein said registration authority transmits encryption algorithm designation information along with said public key certificate issuance request to said certificate authority.*

Claims 14-15 and 17-22

Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on a Registration Authority (RA) and does not disclose a table that associates the registration authority with the assigned encryption algorithm.

On page 18, the **Examiner's Answer** recites that "[t]he Examiner sees the table of the instant application as a representation of an association between a registration authority and a signature algorithm. As such, Vaeth does teach an association between a registration authority and a signature algorithm in the form of a crypto card."

This matter was identical to the one raised with respect to Claims 1-3, 9, 10, 12, and 13, and is refuted for similar reasons.

On page 18, the **Examiner's Answer** also asserts that "[t]he Vaeth patent allows for the *possibility* that the same RA can request different certificates" (Page 17).

It is established precedent that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). Therefore, allowing *for the possibility* of a modification does not meet the requirements of anticipation, or obviousness without proper motivation.

Accordingly, Vaeth fails to teach or suggest a table that associates the registration authority with the assigned encryption algorithm.

- *Thus, Vaeth fails to disclose, teach or suggest causing said certificate authority to select from among a plurality of signature modules each executing a different encryption algorithm , at least one of the signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm for the registration authority, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

Claims 16

In Vaeth, the Certification Authority (CA) produces the type of certificates based on the requesting entities, not based on signature module information from the RA.

On page 19, the Examiner's Answer asserts that "[t]he Vaeth patent allows for the possibility that the same RA can request different certificates. Vaeth states, '[e]ach of the approvals for these three different types of certificates *might be performed* by the same RA 180, for example

the credit card issuer, acting as a different 'virtual CA' (using a different crypto card) for each type of certificate' (Vaeth, column 9, lines 5-9)."

However, in the above passage, Vaeth is not stating that the RA is determining which crypto-card is used. Vaeth simply indicates that each certificate is created using a different crypto card, and a single RA can serve to verify the CRDs data for various types of users. In this same token, Vaeth also discloses that multiple RAs can serve to verify a single type of user. However, in neither case is the specific cypto-card being determined by the RA (Vaeth 7:49-59).

Furthermore, the cited portion of Vaeth disclosing "three different types of certificates" refers to the requesting entities, not the RAs, which Vaeth identifies as "user 170...merchant 177, and payment gateway 178" (Vaeth at 7:34-36).

- *Thus, Vaeth fails to disclose, teach or suggest, wherein said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a encryption algorithm specific to each of said registration authorities.*

Claims 23-26 and 30-35

Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on a Registration Authority (RA).

On page 20, the **Examiner's Answer** maintains that the RA is not a generic entity and that the crypto-card is clearly based on the requesting RA. The Examiner's Answer cites to column 7, lines 23-38 of Vaeth, claiming that Vaeth espressly states that "a Registration Authority (RA) may be associated with a credit card issuer while another RA may be associated with a corporate account authorization office."

This matter was identical to the one raised with respect to Claims 1-3, 9, 10, 12, and 13, and is refuted for similar reasons.

- *Thus, Vaeth fails to disclose, teach or suggest wherein said digital certification apparatus, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with a public key certificate issuance request received from outside said digital certification apparatus and based upon an identification of an assigned encryption algorithm for the registration authority, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.*

Claims 27 stands or falls alone: In Vaeth, the Certification Authority (CA) produces the type of certificates based on the requesting entities, not based on signature module information from the RA.

On page 21, the **Examiner's Answer** maintains that the RA is not a generic entity and that the crypto-card is clearly based on the requesting RA. The Examiner's Answer cites to column 7, lines 23-38 of Vaeth, claiming that Vaeth espressly states that "a Registration Authority (RA) may be associated with a credit card issuer while another RA may be associated with a corporate account authorization office."

This matter was identical to the one raised with respect to Claims 1-3, 9, 10, 12, and 13, and is refuted for similar reasons.

Claims 28 and 29

Vaeth does not disclose using information from the RA to determine which encryption algorithm to use to produce a given type of certificate.

On page 22, the **Examiner's Answer** cites to "column 7, lines 23-28 of the Vaeth patent that expressly states that a Registration Authority (RA) may be associated with a credit card issuer while another RA may be associated with a corporate account authorization office. The RA is not generic entity as alleged by the Applicant.

This matter was identical to the one raised with respect to Claims 1-3, 9, 10, 12, and 13, and is refuted for similar reasons.

On page 22, the **Examiner's Answer** further points out that "'In yet another alternative embodiment, the CA 190 may notify appropriate RAs of its receipt of a CRD [certificate request and data]' (column 8, lines 32-34). It is important to note that the 'appropriate RAs' are notified so that the user submitted data for a certificate request can be verified."

Applicant notes that the role of the RA is simply to provide verification of data (CRD) and, in some cases, relay the information from the entity to the CA. (Vaeth at 8, 36-47). However, the determination of the cryptography is made based on the request received from the entities, not the identity of the RA.

- *Thus, Vaeth fails to disclose, teach or suggest wherein said digital certification apparatus, based on encryption algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated encryption algorithm.*

Claims 36 stands or falls alone: - Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on the requesting Registration Authority (RA).

On page 23, the **Examiner's Answer** recites that "Vaeth states, '[e]ach of the approvals for these three different types of certificates might be performed by the same RA 180, for example the credit card issuer, acting as a different 'virtual CA' (using a different crypto card) for each type of certificate' (Vaeth, column 9, lines 5-9)." However, this portion of Vaeth simply discloses that the

single RA can serve to "approve" different certificates. That is, Vaeth simply indicates that the CRD from the different types of users may be verified by the same RA, acting as different "virtual CA" capacities.

However, in the above passage, Vaeth is not stating that the RA is determining which crypto-card is used. Vaeth simply points out that each certificate type uses a different crypto card, and a single RA can serve to verify the CRDs data for various types of users. In this same token, Vaeth also discloses that multiple RAs can serve to verify a single type of user. However, in neither case is the specific cypto-card being determined by the RA (Vaeth 7:49-59).

- *Thus, Vaeth fails to disclose, teach or suggest selecting, from among a plurality of signature modules each executing a different encryption algorithm, at least one of the signature modules in accordance with a public key certificate issuance request and with reference to a table that associates the registration authority with an assigned encryption algorithm.*

The Final Office Action erroneously rejects claims 4, 7, 26, and 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. (Vaeth) in view of U.S. Patent No. 6,202,157 to Brownlie et al. (Brownlie).

Brownlie discloses a network security system capable of applying security policy provisions issued at a centralized authority to various network nodes, which in turn verify the policy provisions using digital signatures associated with the central authority.

The Examiner's Answer maintains these rejections in light of Examiner's positions with respect to the rejections under 35 U.S.C. § 102. Having refuted these positions, Appellant maintains that Brownlie fails to disclose, teach, or suggest that *said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

The Final Office Action erroneously rejects claims 8, 18, and 30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. (Vaeth) in view of "On the Importance of Checking Cryptographic Protocols for Faults" by Boneh et al. (Boneh).

The Examiner's Answer maintains these rejections in light of Examiner's positions with respect to the rejections under 35 U.S.C. § 102. Having refutd these positions, Appellant maintains that Boneh fails to teach or suggest the distribution of encrypted certificates.

- *Thus, Boneh fails to disclose, teach, or suggest that said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

The Final Office Action erroneously rejects claims 11, 21, and 33 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,035,402 to Vaeth et al. (Vaeth) in view of U.S. Patent No. 6,675,296 to Boeyen et al. (Boeyen).

The Examiner's Answer maintains these rejections in light of Examiner's positions with respect to the rejections under 35 U.S.C. § 102. Having refutd these positions, Appellant maintains that Boeyan fails to teach or suggest a certification scheme or associating a registration authority with an encryption algorithm

- *Thus, Boeyen fails to disclose, teach, or suggest that said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm.*

Conclusion

The claims are considered allowable for the reasons discussed above, as well as for the additional features they recite.

Reversal of the Examiner's decision is respectfully requested.

If any fee is required or any overpayment made, the Commissioner is hereby authorized to charge the fee or credit the overpayment to Deposit Account # 18-0013.

Dated: January 23, 2008

Respectfully Submitted,

By 40,290

Christopher M. Tobin
Registration No.: 40,290
Ronald P. Kananen
Registration No.: 24,104
RADER, FISHMAN & GRAUER PLLC